

Document Creator: Dave Sigler

Date Created: January 18, 2014

Approver(s): KIDS Leadership

Date Approved: February 14, 2014

I. Overview

Summary: The document establishes a KETS Recommended and Approved Approach to extend the District Network to remote locations. Users connecting on the remote network will be protected by the same technology protection measures in place for the School District's Private Network.

Purpose and Scope: This Document is to define a method to extend the District Network to remote sites by implementing IPsec VPN Tunneling between the two sites. This is commonly referred to as ***Site-to-Site Tunneling***. Technical design and implementation guidelines, strategies, and implementation considerations are included in this Document.

Reason for Implementing: The Office of Knowledge, Information and Data Services (KIDS) has a vested interest in ensuring School Districts have the tools necessary to implement and enforce the Individual District's Internet Safety Policy. Many Districts have asked for guidance on how to implement technology protection measures on devices not directly connecting to the District Network.

District Scenarios: Many Districts are identifying remote locations that need to be part of the District Network. Examples include:

- School Buses with mobile appliances installed that include Wi-Fi Hotspot functionality.
- Bus Garage with Broadband Internet Service such as Cable or DSL.
- Portable Wi-Fi Hotspot for temporary or permanent use off site.

II. Definitions

Broadband	High Speed Internet data connection from Cable or DSL Service Provider. For the purpose of this document, Cellular Wireless Connections will be considered Broadband.
IPsec VPN Tunnel	An encrypted logical connection between two networks that makes them appear directly connected to each other. Data that enters one end of the Tunnel comes out the other end. This is accomplished by using:
VPN Appliance	A device capable of providing one end of a VPN Tunnel. It has a WAN port used to connect to the Internet and establish a Tunnel. It has a LAN port to connect to the remote network or District LAN.
Remote VPN Appliance	<p>Connects to the Remote Broadband Provider and the Remote LAN. In the case of a Wi-Fi hotspot, the VPN Appliance Capability must be built in.</p> <p>The Appliance is typically implemented as part of an all-in-one device. As such, the VPN Appliance may be purchased from a KETS Contract or through other Procurement Channels.</p>
VPN Concentrator	<p>VPN Appliance designed to handle Tunnels to multiple remote sites. The WAN port of the Concentrator will connect to the DMZ Switch in the KEN Rack. It will establish the Tunnel(s) to the Remote Appliances. The LAN port will connect to the District Network and serve as the entry point into the Network from the remote locations.</p> <p>In order for the VPN Concentrator to work properly, a ticket will need to be opened with the KETS Service Desk to:</p> <ul style="list-style-type: none">• Set up the Firewall Rules to allow this service.<ul style="list-style-type: none">○ District must agree to a cooperative support model which may require administrative access be granted to this device (and any device connected to the KETS local DMZ), and acknowledges traffic or service concerns could result in the temporary disabling of the service.• Identify the port to use on the DMZ Switch for the WAN Interface. <p>The VPN Concentrator should be purchased from a KETS Contract.</p>

The VPN Concentrator shall not be installed in the KEN Rack or use KEN Rack Power.

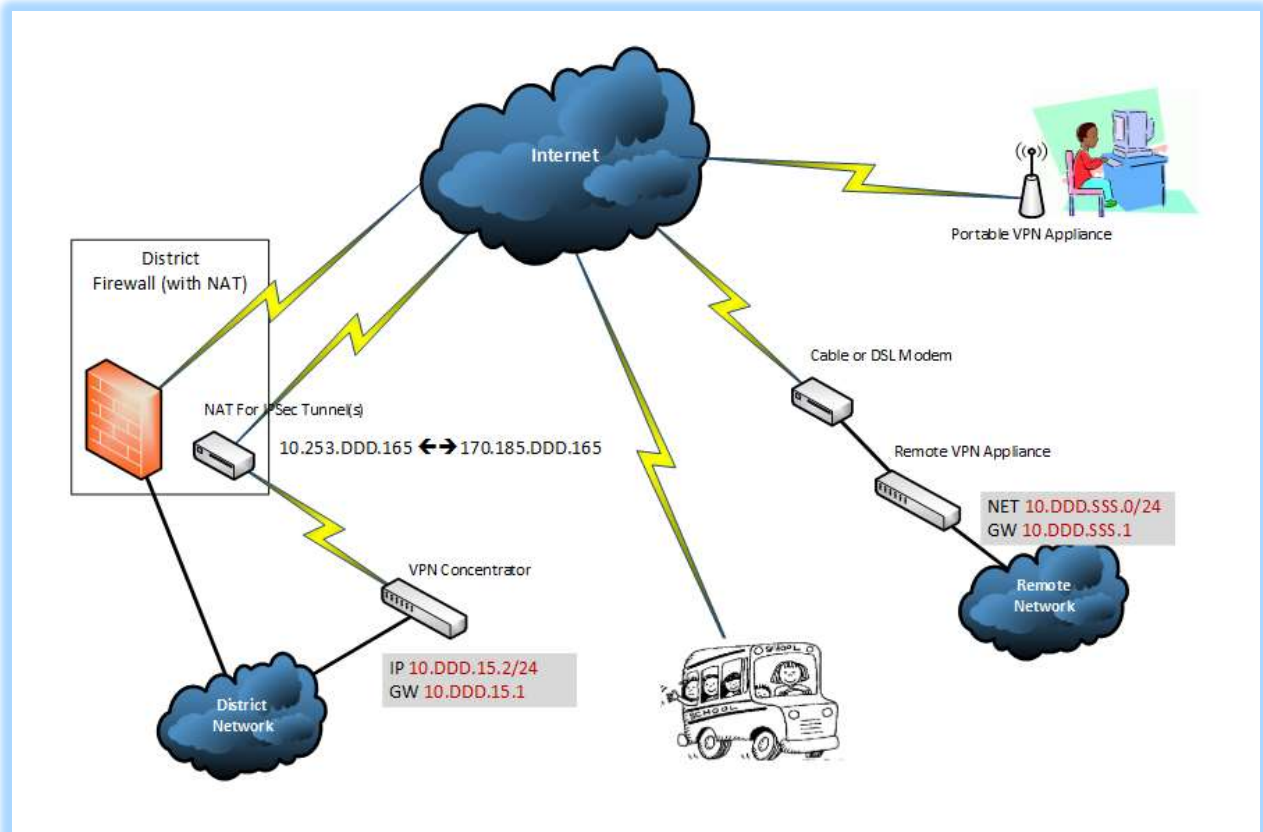
Static Public IP

The Broadband Service Provider must be able to provide a static public IP. This is an Internet Protocol (IP) address that is publicly routable. The address must be static in that once assigned and used, changing it will corrupt the Tunnel Configuration.

III. Functionality

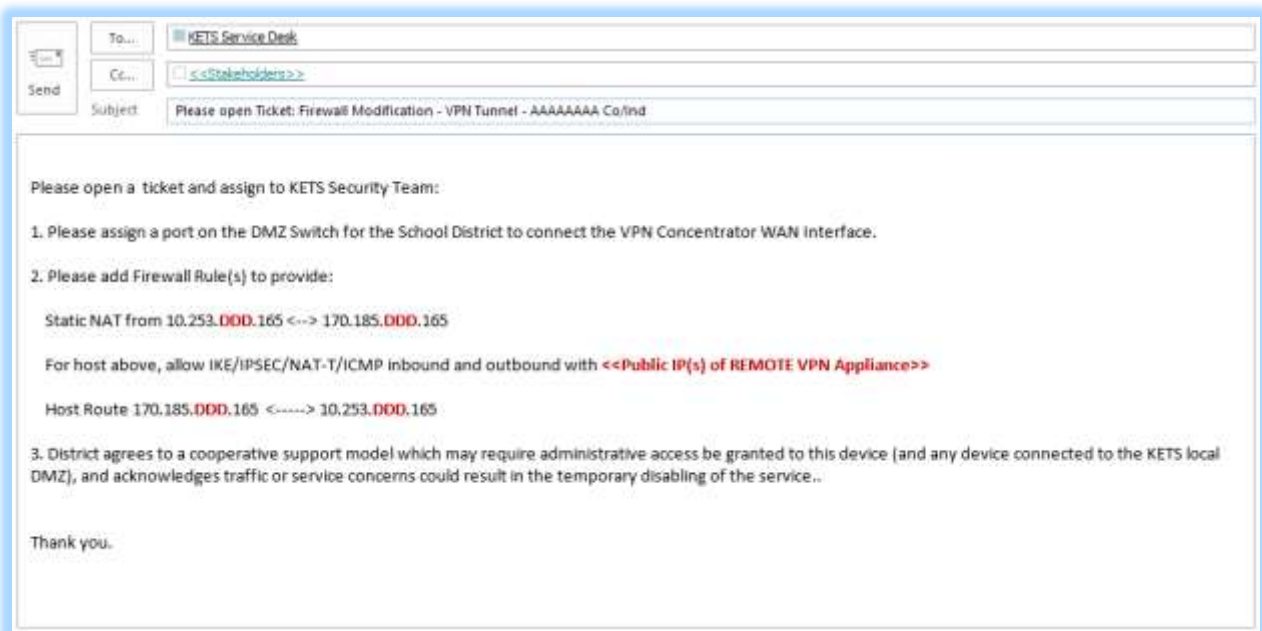
Please review the diagram below.

- Traffic is generated from a remote user.
 - ...with a Private IP Address from the District's Address Pool.
- Traffic from the remote user enters the Remote VPN Appliance
- The traffic travels through the VPN Tunnel to the VPN Concentrator.
- It enters the District Network from the VPN Concentrator's LAN Interface
- It is treated like any other District traffic.
- When return traffic for the remote user hits the District Network it is forwarded to the VPN Concentrator for delivery back through the Tunnel.



IV. Implementation Process

1. (Recommended) Unless the District has the technical expertise on staff, identify a KETS Vendor Partner who will provide design assistance, initial installation & configuration, and ongoing support for these remote services. The KETS Contract provides the vendor flexibility to structure a variety of Support Models.
2. Identify the VPN Concentrator, Remote Broadband Service, and Remote VPN Appliance(s) to be implemented.
3. Identify the Static Public IP(s) of the Remote VPN Appliances.
4. Open a ticket with the KETS Service Desk to allow the VPN Concentrator Service. (See example below.) Allow for three (3) business days for the Service to be enabled.
5. Install and configure Service.



The screenshot shows a web-based form for submitting a ticket to the KETS Service Desk. The form includes fields for 'To...' (KETS Service Desk), 'Cc...' (<<Stakeholders>>), and 'Subject' (Please open Ticket: Firewall Modification - VPN Tunnel - AAAAAAAA Co/Ind). Below these fields is a large text area containing the following text:

Please open a ticket and assign to KETS Security Team:

1. Please assign a port on the DMZ Switch for the School District to connect the VPN Concentrator WAN Interface.
2. Please add Firewall Rule(s) to provide:

Static NAT from 10.253.DDD.165 <--> 170.185.DDD.165

For host above, allow IKE/IPSEC/NAT-T/ICMP inbound and outbound with <<Public IP(s) of REMOTE VPN Appliance>>

Host Route 170.185.DDD.165 <-----> 10.253.DDD.165
3. District agrees to a cooperative support model which may require administrative access be granted to this device (and any device connected to the KETS local DMZ), and acknowledges traffic or service concerns could result in the temporary disabling of the service..

Thank you.